Re:Purpose

Fair Ordering & Entropy via Bitcoin Weak Blocks

Abstract

*Re:Purpose introduces a novel, decentralized protocol leveraging Bitcoin's discarded near-miss hashes ("weak blocks") to establish a **trustless, verifiable fair ordering mechanism with capped participation**. By tiering weak blocks by difficulty and sorting user commitments by hash proximity, the protocol enables dApps to securely sequence transactions, mint NFTs, run lotteries, and anchor messages with inherent resistance to front-running, MEV, and Sybil attacks—all without trusted intermediaries.*

Introduction

Fair ordering in decentralized systems with capped user participation remains an open problem, crucial for NFT drops, auctions, DAO voting, and other time-sensitive applications. Existing methods suffer from front-running, censorship, or reliance on trusted sequencers. Re:Purpose solves this by transforming Bitcoin's wasted proof-of-work entropy into a multi-tiered, economically sustainable token system ($RPRP), providing a **naturally scarce and auditable ordering substrate**.

Technical Overview

Weak Block Tier System

Bitcoin miners continuously produce "weak blocks" — cryptographic hashes that are near but above the current difficulty target. Re:Purpose leverages this discarded computational work by classifying these weak blocks into distinct tiers (Gold, Silver, Bronze, Copper), where each subsequent tier is approximately 16 times more frequent than the previous one. This tiered architecture enforces a **hard cap on entries per interval**, effectively bounding participation levels and enabling inherent fairness in the system.

Ordering Mechanism

The protocol operates through a commitment-based submission system where users submit cryptographic commitments linked to their transaction data. Ordering within each tier is deterministically established by measuring hash proximity to the Bitcoin difficulty target, ensuring a **neutral, verifiable sequence that cannot be manipulated through timing attacks or fee manipulation**. The system employs commit-reveal schemes as an additional layer of protection against front-running attacks.

Token Economics & Incentives

The economic model centers around miners minting $RPRP tokens in proportion to the difficulty of the weak blocks they submit to the protocol. Users can spend these $RPRP tokens to secure either "Secure Slots" for guaranteed inclusion in the ordering system or "Chance Entries" for probabilistic inclusion based on available capacity. The fee structure distributes revenues across multiple stakeholders, with portions allocated to miners as incentives, token burning for deflationary pressure, and ecosystem growth reserves to sustain long-term protocol development.

Cross-Chain Anchoring

To enable real-time verification and maintain auditability, weak block metadata is anchored within Solana smart contracts, providing fast access to Bitcoin's entropy without requiring direct blockchain queries. This cross-chain architecture enables decentralized applications to reference Bitcoin's proof-of-work entropy in real-time while maintaining cryptographic guarantees of authenticity and temporal ordering.

Use Cases

- **Capped NFT Minting:** Fairly ordered, anti-front-run sales with strict supply limits.
- **DAO Timelocks and Vaults:** Unlock actions triggered by secure tiered events.
- **Decentralized Messaging:** IPFS-based E2EE messaging anchored with timestamped weak block proofs.
- **Randomness and Lotteries:** Tiered entries enable provably fair draws.

Challenges & Next Steps

- Miner plugin adoption and network coverage are critical for security.
- UX and developer tooling must simplify commitment submission and proof verification.
- Economic parameters (tier sizes, fees) require tuning and governance.
- Future work includes formal security proofs, simulations, and pilot dApps.

Conclusion

Re:Purpose pioneers a fundamentally new approach to fair ordering and entropy sourcing, turning Bitcoin's wasted hashes into a public good substrate for next-generation decentralized applications.

For detailed protocol specs, economic models, and implementation roadmap, please contact the Re:Purpose team.